

## **IN THE CLAIMS**

This listing of claims will replace all prior versions and listings of claims in the application.

1. (Currently amended) A method of preventing theft of an organization property, comprising:  
  
storing first identification information of an organization property;  
  
collecting second identification information of the organization property;  
  
comparing the second identification information with the first identification information to generate authentication result; and  
  
~~a. generating an authentication result from comparing stored identification information with collected identification information of the organization property; and~~  
  
~~b. transmitting a plurality of types of network packets containing the authentication result to a plurality of organization servers via a network.~~
2. (Currently amended) The method according to claim 1, wherein comparing the second identification information with the first identification information~~1(a)~~ further comprises:  
  
retrieving the first~~stored~~ identification information and network addresses of the organization servers from a tamper-resistant storage location.
3. (Currently amended) The method according to claim 2, wherein transmitting the plurality of types of network packets~~1(b)~~ further comprises:

assembling the plurality of types of network packets with the network addresses and with information indicative of a current location of the organization property.

4. (Currently amended) The method according to claim 3, further ~~comprising~~ comprises:
  - a. assembling and transmitting an intranet network packet to an intranet server; and
  - b. ~~in response to non-acknowledgement from the intranet server~~, assembling and transmitting an ~~Internet~~ internet network packet to an ~~Internet~~ internet server in response to a non-acknowledgement from the intranet server.
5. (Currently amended) The method according to claim 2, further ~~comprising~~ comprises:  
retrieving the ~~second collected~~ second collected identification information from the organization property.
6. (Currently amended) The method according to claim 2, further ~~comprising~~ comprises:  
retrieving the ~~second collected~~ second collected identification information from an electronic system that contains the organization property.
7. (Currently amended) The method according to claim 5, wherein the ~~second collected~~ second collected identification information comprises an Internet Protocol address assigned to the organization property.

8. (Currently amended) The method according to claim 6, wherein the ~~second~~ collected identification information comprises device identification information of the electronic system.
9. (Currently amended) A machine readable medium having embodied thereon instructions, which when executed by a machine, causes the machine to perform a method of preventing theft of an organization property, the method~~instructions~~ comprising:
- storing a first identification information of an organization property;
- collecting a second identification information of the organization property;
- comparing the second identification information with the first identification  
information to generate an authentication result; and
- ~~a. generating a authentication result from comparing stored identification information~~  
~~with collected identification information of the organization property; and~~
- ~~b.~~ transmitting a plurality of types of network packets that are indicative of the authentication result to a plurality of organization servers via a network.
10. (Currently amended) The machine readable medium according to claim 9, ~~the~~  
~~instructions for 9(a)~~ wherein comparing the second identification information with the  
first identification information further comprises:
- retrieving the first~~stored~~ identification information and network addresses of the organization servers from a tamper-resistant storage location.

11. (Currently amended) The machine readable medium according to claim 10, wherein  
transmitting the plurality of types of network packets~~the instructions for 9(b)~~ further  
comprises:  
  
assembling the plurality of types of network packets with the network addresses and  
information indicative of a current location of the organization property.
12. (Currently amended) The machine readable medium according to claim 11, the  
method~~instructions~~ further comprising~~including~~:  
  
a. assembling and transmitting an intranet network packet to an intranet server; and  
  
b. ~~in response to non-acknowledgement from the intranet server,~~ assembling and  
transmitting an Internet~~internet~~ network packet to an Internet~~internet~~ server in response to  
a non-acknowledgement from the intranet server.
13. (Currently amended) The machine readable medium according to claim 10, the  
method~~instructions~~ further comprising~~including~~:  
  
retrieving the second~~collected~~ identification information from the organization  
property.
14. (Currently amended) The machine readable medium according to claim 10, the  
method~~instructions~~ further comprising~~including~~:

retrieving the ~~secondecollected~~ identification information from an electronic system that contains the organization property.

15. (Currently amended) The machine readable medium according to claim 13, wherein the ~~secondecollected~~ identification information comprises an Internet Protocol address assigned to the organization property.
16. (Currently amended) The machine readable medium according to claim 14, wherein the ~~secondecollected~~ identification information comprises device identification information of the electronic system.
17. (Currently amended) A theft prevention system for detecting theft of an organization property, comprising:
  - a. a plurality of organization servers coupled to a network;
  - b. a tamper-resistant storage location to maintain a firststored identification information of the organization property and network addresses of the organization servers;
  - c. a theft monitor, coupled to the tamper-resistant storage location, to generate an authentication result by comparing the firststored identification information with a ~~secondecollected~~ identification information of the organization property; and
  - d. a network access controller, coupled to the theft monitor, to transmit a plurality of types of network packets containing the authentication result to the organization servers via the network.

18. (Currently amended) The theft prevention system according to claim 17, the theft monitor further to assemble~~further assembles~~ the plurality of types of network packets with the network addresses and with information indicative of a current location of the organization property.
19. (Currently amended) The theft prevention system according to claim 18, the theft monitor further:
- a. to transmits an intranet network packet to an intranet server; and
  - b. in response to a non-acknowledgement from the intranet server, to transmits an Internet~~internet~~ network packet to an Internet~~internet~~ server.
20. (Currently amended) The theft prevention system according to claim 18, the theft monitor further:
- a. to causes the network access controller to transmit an intranet network packet to an intranet server; and
  - b. in response to a non-acknowledgement from the intranet server, to causes the network access controller to transmit an Internet~~internet~~ network packet to an Internet~~internet~~ server.

21. (Currently amended) The theft prevention system according to claim 17, the theft monitor further to retrieves the collected identification information from the organization property.
22. (Currently amended) The theft prevention system according to claim 17, the theft monitor further to retrieves the collected identification information from an electronic system that contains the organization property.
23. (Currently amended) The theft prevention system according to claim 21, wherein the ~~second~~collected identification information comprises an Internet Protocol address assigned to the organization property.
24. (Currently amended) The theft prevention system according to claim 22, wherein the ~~second~~collected identification information comprises device identification information of the electronic system.